Records Retention Schedule

Standard ID
IOT-CS-OPS-005

Published Date
11/1/2016

Effective Date
11/1/2016

Last Updated
10/31/2016

Next Review Date
10/31/2017

Policy
11.0 Protective Technology (PR.PT)
       11.1 PR.PT-1
              11.1.1 Audit/Log Records

Purpose
An approved Records Retention and Disposition Schedule grants agencies the authority to transfer or destroy records on a continuing basis.

Scope
IOT

Statement
In accordance with the State Agency Records Retention and Disposition Schedule, records must be retained and destroyed for a period commensurate with the approved Retention Period. The following are the requirements for IOT:

Title/Description	Retention Period
Operations	
Request for Change (RFC)/ Change Management Request (CMR)	DESTROY after three (3) calendar years
Request for Change (RFC)/ Change Management Request (CMR) Supporting Documentation	DESTROY after one (1) calendar year
Backup Schedules and Reports	DESTROY after one (1) calendar year
User Access Request	DESTROY three (3) years after termination or deletion of the user's access
User Access Control List	DESTROY one (1) calendar quarter after a new list has been produced
System Event Logs	DESTROY after one (1) calendar quarter
Performance Log	DESTROY after one (1) calendar quarter
Database Documentation	DESTROY three (3) calendar years after documentation has been updated or replaced
System Documentation	DESTROY three (3) calendar years after documentation has been updated or replaced
Data Service Orders (DSO)	DESTROY three (3) years after all service work ordered is completed and after receipt of State Board of Accounts Audit Report and satisfaction of unsettled charges

RSA Archer eGRC

Telephone Service Orders (TSO)	DESTROY three (3) years after all service work ordered is completed and after receipt of State Board of Accounts Audit Report and satisfaction of unsettled charges
System Backups – Application Data	DELETE/DESTROY after three (3) calendar years
System Backups – System State Data	DELETE/DESTROY after one (1) calendar year
Master File and Database Backups	DELETE/DESTROY after three (3) calendar years or when agency's original records have been deleted in accordance with their applicable records retention schedule
IN.gov	
www.IN.gov Website Pages	At the end of each fiscal year, TRANSFER all website pages on a formatted medium to the STATE ARCHIVES for permanent archival retention
www.IN.gov Calendar Data	TRANSFER to the STATE ARCHIVES for EVALUATION, SAMPLING and WEEDING pursuant to archival principles, one (1) year after the end of the calendar year covered by the data. DELETE agency copy of data after transfer and when no longer required for internal Office of Technology research purposes
www.IN.gov Statistical Data	
Customer Service Center – Help Desk/Incident Management	
Problem Management Tickets	DESTROY after three (3) calendar years
Problem Management Reports	DESTROY after one (1) calendar quarter
Security	
Security Reports	RETAIN for the duration of investigation. Upon satisfaction of any disciplinary action arising from report, TRANSFER employee-specific records to PERSONNEL FILE (GRPER-5) at the employing agency. At that time, the records are subject to disclosure to affected employees. DESTROY one (1) year after report date if agency has determined that monitoring reveals nothing that will be used in a disciplinary action
Security Assessments	TRANSFER to the RECORDS CENTER after two (2) fiscal years and after receipt of State Board of Accounts Audit Report and satisfaction of unsettled charges. DESTROY in the RECORDS CENTER after an additional eight (8) fiscal years. TOTAL RETENTION: ten (10) fiscal years
Information Resources User Agreement (IRUA)	DESTROY three (3) years after termination or deletion of the user's access
Incident Response	DESTROY five (5) years after date of incident
Disaster Recover/Continuity	
Off-Site Backup Media and Documentation	Destroy when outdated or replaced
Disaster Recovery and Continuity Training Plan	Destroy ten (10) years after plans are outdated or replaced
Disaster Recovery and Continuity Training Test	Destroy when outdated or replaced
Project Management	
Project Documentation	TRANSFER to the RECORDS CENTER three (3) years after conclusion of the project detailed in the related Statement of Work, after receipt of State Board of Accounts Audit Report and satisfaction of unsettled charges. DESTROY after an additional seven (7) years in the RECORDS CENTER. TOTAL RETENTION: ten (10) years plus receipt of State Board of Accounts Audit Report and satisfaction of unsettled charges
GMIS	
Change Requests Log	DESTROY one (1) year after decommission of the related software application

Roles

All Personnel

Responsibilities

All personnel must be aware of the retention period requirements, governing teams must act in accordance with the published retention schedule.

Management Commitment

Management shall read and understand the retention requirements related to their records, and act accordingly with this Standard.

Coordination Among Organizational Entities

All personnel shall work with appropriate IOT teams to understand and satisfy requirements related to the approved records retention and disposition schedule.

Compliance

Management may request reporting for specific records to validate compliance.

Exceptions

Exceptions will be handled on a case by case basis through the Chief Operational Officer or delegate.

Associated Documents

State Agency Records Retention and Disposition Schedule